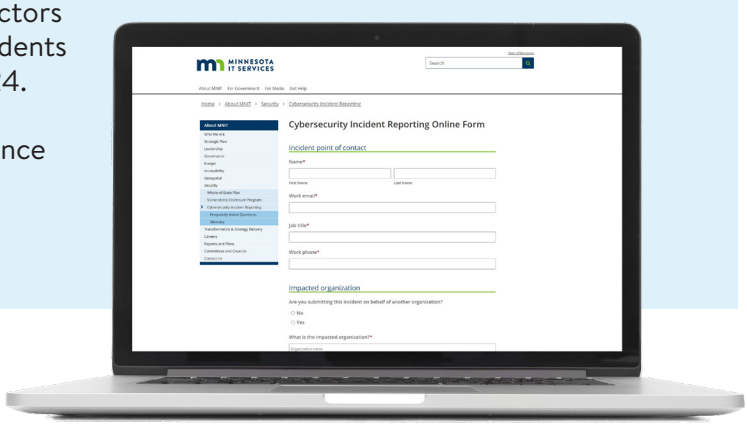
MINNESOTA IT SERVICES

Cybersecurity Incident Reporting

Public agencies in Minnesota and supporting contractors or vendors are required to report cybersecurity incidents that impact their organization beginning Dec. 1, 2024.

The requirement, included in state law, aims to enhance cyber defenses by collecting information about cybersecurity incidents, anonymizing it, and sharing it with appropriate organizations.



How to report a cybersecurity incident

Report a cybersecurity incident using the form on Minnesota IT Services' (MNIT) website: mn.gov/mnit/cir.

The form, which is the preferred and most time-efficient method for reporting, will:

- Take no longer than five minutes to complete, depending on details provided.
- Route incidents involving criminal justice information to the Minnesota Bureau of Criminal Apprehension (BCA).
- Route incidents involving election infrastructure to the Office of the Minnesota Secretary of State.

If you cannot access the form or need immediate attention, use one of these options:

- Call the MNIT Enterprise Service Desk: 651-297-1111 or 1-888-717-6638 for help completing the form.
- Email the MNIT Cyber Navigator Team at CN.MNIT@state.mn.us and include a phone number for the CN team to contact you and assist in completing the form.

Requirements

Who must report

State agencies; political subdivisions; K-12 school districts, charter schools, intermediate districts, cooperative units, and public post-secondary (higher education) institutions. Government contractors or vendors that provides goods or services to a public agency must report an incident to the public agency, who in turn is required to submit a report.

What must be reported

A cybersecurity incident is defined by law as an action taken using an information system or network that results in an actual or potentially adverse effect on an information system, network, or the information it contains. Find more information on the MNIT Cyber Incident Reporting site: **mn.gov/mnit/cir**.

When reports must be made

Within 72 hours of when an incident was identified or occurred, or within 24 hours if criminal justice information may be impacted.

Benefits

Cybersecurity threats are increasingly damaging to government operations and are an evolving public safety risk. By working together to understand Minnesota's cyber-threat landscape, we strengthen our state's cyber-resilience, protect critical systems, and keep data secure.

Minnesotans

- Gain a better understanding of the nature of and impacts from cybersecurity events to keep services available to Minnesotans and protect their data.

Public entities

- Gain access to MNIT and BCA's shared cybersecurity threat advisories and general guidance to help defend against cybersecurity threats.
- Are better equipped to identify potential gaps that require resources to mitigate risk.

MNIT and BCA

- Gain awareness of the scope of incidents and can better assist organizations in defending their IT resources.
- Understand how bad actors bypass security controls; and can better identify trends.

MNIT, the BCA, and Minnesota Fusion Center appreciate your partnership in taking sensible steps to secure Minnesota.

Protecting information

A cybersecurity incident report is considered security information pursuant to Minnesota Statute 13.37. Reports are not discoverable in a civil or criminal action, absent a court order or a search warrant, and are not subject to subpoena. MNIT may anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks on other entities. MNIT will contact the reporting entity prior to anonymizing and sharing information.

More information

Reporting instructions, guidance, types of cybersecurity incidents to report, and answers to frequently asked questions are available on MNIT's website: **mn.gov/mnit/cir**.